CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)

Applicant(s): **DiSanto**

Docket No.
COPY-62

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit
09/782,860	**2/14/2001**	**Andrew L. Nalvern**	**45722**	**2134**

Invention: **METHOD AND SYSTEM FOR SELECTING ENCRYTION KEYS FROM A PLURALITY OF ENCRYPTION KEYS**

I hereby certify that the following correspondence:

Appeal Brief (9 pgs), Appendix I (1 pg.), Appendix II (1 pg.), Appendix III (1 pg.), Table of Contents (1 pg.), copy of Amendment After Notice of Appeal (3 pgs).

(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

09/12/2005
(Date)

Edna Schmitinger
(Typed or Printed Name of Person Mailing Correspondence)

Edna Schmitinger
(Signature of Person Mailing Correspondence)

EV584652118US
("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

Applicant	:	Disanto et. al
Serial No.	:	09/782,860
Filed	:	February 14, 2001
For	:	Method and System for Selecting Encryption Keys From a Plurality
	:	of Encryption Keys
Examiner	:	Andrew L. Nalvern
Art Unit	:	2134

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

May It Please The Honorable Board:

This is Appellants' Brief on Appeal from the final rejection of claims 1 – 32, Appellants having filed a Notice of Appeal received in the U.S. Patent Office on July 14, 2005. Appellants waive an Oral Hearing for this appeal.

The Office is authorized to charge any fees due and owing, or credit any overpayment, to Deposit Account No. 50-3208. Enclosed is a single copy of this Brief.

I. REAL PARTY IN INTEREST

The real party in interest of Application Serial No. 09/782,860 is the Assignee of record:

Copytele, Inc.
900 Walt Whitman Road
Melville, New York 11746

I hereby certify that this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to Mailstop Appeal Brief – Patents, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature

EDNA SchmiTTINbeR
Name

II. RELATED APPEALS AND INTERFERENCES

There are currently, and have been, no Appeals or Interferences regarding Application Serial No. 09/782,860 known to the undersigned attorney.

III. STATUS OF THE CLAIMS

Claims 1 - 32 are rejected. Claims 2 – 32 have been cancelled, without prejudice, in an amendment filed contemporaneously herewith. A copy of this Amendment has been attached hereto. Accordingly, the rejection of Claim 1 is appealed.

IV. STATUS OF AMENDMENTS

All amendments were entered and are reflected in the claims included in Appendix I.

V. SUMMARY OF CLAIMED SUBJECT MATTER

This summary sets forth exemplary reference characters and pages and line numbers in the specification. The identification of reference characters and pages and line numbers does not constitute a representation that any claim element is limited to the embodiment illustrated at the reference character or described in the referenced portion of the specification.

Independent Claim 1 recites a method to encrypt a data message having a plurality of message data blocks prior to transmitting said message data blocks over a network (Fig. 3, page 7, lines 4-5; see also, page 3, lines 19-20, page 5, lines 2-8). The claimed method includes extracting a data value from one of the message data blocks (Fig. 3, step 410, page 7, lines 9-11; see also, page 6, lines 3-9). The claimed method includes selecting an encryption key from among a plurality of encryption keys dependently upon the extracted data value (Fig. 3, elements 415/465, 420/455, 425/445 and 435, page 7, line 19 – page 8, line 16; see also page 7, lines 12-14, lines 19-21). The claimed method includes encrypting a subsequent one of the message data blocks using the selected encryption key (Fig. 3, elements 470, 460, 450, 440, page 7, line 19 – page 8, line 16; see also, page 5, lines 14-18).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner has rejected Claim 1 as being anticipated under 35 USC 102(b) by Matsui (U.S. Pat. No. 5,488,661).

VII. ARGUMENT

The invention as recited in claim 1 is not anticipated by Matusi, as Matsui fails to disclose each of the limitations recited in claim 1.

I. Anticipation Requires That Each And Every Element Set Forth In A Claim Is Found In A Prior Art Reference.

In order to anticipate, a prior art reference must describe the same invention as is recited by the subject claim. *See, e.g., Glaverbel Societe Anonyme v. Northlake Marketing & Supply, Inc., 45 F.3d 1550, 33 U.S.P.Q.2d 1496, 1498 (Fed. Cir. 1995).* That is, "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *See, M.P.E.P. §2131 citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987).* Thus, unless the identical invention as that claimed is shown in as complete detail as is contained in the claim, the claim is not anticipated. *See, e.g., Richardson v. Suzuki Motor Co., 9 USPQ.2d 1913, 1920 (Fed. Cir. 1989).* Accordingly, if Matsui fails to teach even one element of Claim 1 of the subject application, Matsui fails, as a matter of law, to anticipate Claim 1.

II. Claim 1 Recites A Method That Uses A Previous Data Block's Content To Select An Encryption Key For A Subsequent Data Block

It is desirable to encrypt sensitive data, such as business strategy, credit card numbers, social security numbers or bank account balances, prior to transmitting them over a network. *See, e.g., Specification, page 1, lines 12- 16.* Applicant acknowledges that methods for encrypting data are generally known. Applicant further acknowledges that data transmission networks commonly use message data blocks, *e.g.*, a series of data elements handled as a single unit, or a unit of data, to transmit information. However, the claimed invention uses the contents of a previous message data block to select an encryption key for encrypting a subsequent message data block – an approach distinct from that taught by Matsui.

The preamble of Claim 1 recites, "[a] method to encrypt a data message having a plurality of message data blocks prior to transmitting said message data blocks over a network." An exemplary block-diagram illustrating such a process is shown in Fig. 3 of the subject application.

The claimed method comprises "extracting a data value from one of said message data blocks." This is explained in the subject application, with reference to Fig. 3, and the accompanying text, which recites that "the transmitting party extracts a known number of bits from a known position within a message data block at step 410". *Specification, page 7, lines 9-11.* By way of further, non-limiting explanation, this step is also discussed on page 6, in lines 3-7 of the subject application, which discloses that the last data byte of a message data block may be extracted.

The claimed method further comprises, "selecting an encryption key from among a plurality of encryption keys dependently upon said extracted data value." This is explained in the subject application, again with reference to Fig. 3, by the accompanying text which teaches that encryption codes are selected at steps 465, 455, 445, 435 based upon comparing the extracted data to some predetermined criteria. *See, Specification, page 7, line 19 – page 8, line 16 ("[a]t block 415 a determination is made whether the value of the extracted data is less than four. If the determination is in the positive, then one of the encryption keys is selected, at block 465 ... ").*

Finally, the claimed method comprises "encrypting a subsequent one of said message data blocks using said selected encryption key" (emphasis added). This is explained in the subject application, again with reference to Fig. 3, by the accompanying text, wherein "a transmitting party transmits an encrypted message block ... using an encryption key represented as E(x). ... In [the] illustrative embodiment of the invention encryption key E(x) is determined from the data content of a previous message block". *Specification, page 5, lines 14-17.*

In order to anticipate Claim 1 of the subject application, Matsui must disclose each of the above-identified limitations, including the limitation wherein a subsequent message data block is encrypted using an encryption key selected on the basis of the content of a previous message block.

III. Matsui Teaches A Method That Uses 8-Bytes Of Input Data To Select Encryption Keys For The Same 8-Bytes Of Input Data

Matsui fails to disclose or suggest any encryption dependence between previous and subsequent message data blocks of a data message as is recited in present claim 1. Instead, Matsui teaches dividing a single instantiation of 8-bytes of message data into more and less significant portions, and encrypting those same 8-bytes of message data using keys selected on the basis of the then less significant portion. Matsui's use of portions of the 8-bytes of input data to select encryption keys for those same 8-bytes of input data can not be interpreted to somehow equate to Applicant's claimed method of using data extracted from a previous message data block to select a key for encrypting a subsequent message data block of a data message.

The Final Office action mailed April 15, 2005 argues:

> "Matsui teaches that a second processing block encrypts a second input data by using a key selected dependently upon the 4 less significant bits of the previous processing block's output (Matsui, column 6 lines 17-35)." *See 4/15/2005 Office action, page 2, par. 4.* emphasis added.

The Final Office action further argues on page 3, para. 8 that

> "Matsui teaches the extracting of a data value from a message data block (Matsui, column 5 line 67 - column 6 line 4, selects less significant 4 bytes), the selecting of an encryption key from among a plurality of encryption keys dependently upon said extracted data value (Matsui, column 6 lines 17 - 35, extended key), [and] encrypting a subsequent message data block using the selected encryption key (Matsui, column 6 lines 17-35).

Applicant traverses these assertions. First, a detailed reading of the relied upon passages reveals that Matsui inputs 8-bytes of plaintext designated as numeral 3 in Fig. 1 of Matusi. Matsui divides these 8-bytes of input data into more and less significant portions (i.e. the 4 more significant bytes and the 4 less significant bytes). *See, e.g., U.S. Patent No. 5,488,661, col. 5, line 67 – col. 6, line 1.* Matsui then calculates an address based upon the less significant portion of the 8-bytes of input data 3. *See, e.g., U.S. Patent No. 5,488,661, col. 6, lines 4- –7.* Matsui then supplies a key selected using the calculated address to a first processing block 9. *See, e.g., U.S. Patent No. 5,488,661, col. 6, lines 7 – 9.* Processing block 9 of Matsui uses the scrambling key to scramble the <u>same</u> less significant byte portion that was used to select the scrambling key in the first place. *See, e.g., U.S. Patent No. 5,488,661, col. 6, lines 10 - 13.* Matsui then exclusive ORs the scrambled less significant portion with the more significant portion of the 8-bytes of input data. *See, e.g., U.S. Patent No. 5,488,661, col. 6, lines 13 - 14.* Finally, the resultant and the less significant portion replace one another. *See, e.g., U.S. Patent No. 5,488,661, col. 6, lines 15 - 67 – col. 6, lines 14 - 16.*

The output therefore consists of the calculated result (based upon XORing the more significant byte portion and the scrambled less significant byte portion) and the less significant byte portion of the 8-bytes of input data, and is input to the second block 10 (see, e.g., Fig. 2, where the single 2 byte input data block includes 1 more significant byte (FF) and 1 less significant byte (00), and processing block 10 receives (FF), (00) from processing block 9). *See, e.g., U.S. Patent No. 5,488,661, col. 6, line 66 – col. 7, line 1.*

Scrambling block 10 uses the output of block 9 in an analogous manner to provide an output to processing block 11, which operates in an analogous manner to provide an output to processing block 12, and so on. Eventually, in response to the 8 bytes of plaintext input 3, Matsui provides 8-bytes of scrambled output 4. *See, e.g., U.S. Patent No. 5,488,661, Figs. 1 and 2; col. 5, lines 44 - 46.*

Thus, Matsui merely uses *a sequence of processing blocks (e.g., processing blocks 9 – 16)* to scramble *8 –bytes of input data 3* using keys ultimately selected on the basis of that very *same single 8-bytes of input data* (i.e., the 4 less significant bytes in the single message block at the corresponding processing block). Accordingly, Matsui does not teach "extracting a data value from one of said message data blocks; selecting an encryption key from among a plurality of encryption keys dependently upon said extracted data value; and, encrypting a subsequent one of said message data blocks using said selected encryption key" as recited in claim 1, as the 8-bytes of input data 3 of Matsui are scrambled solely on the basis of their own data values.

In an effort to further support this rejection, the Advisory action mailed June 22, 2005 argues,

> Matsui teaches a data block that is encrypted with a key that is dependently chosen based on a previous data block. The two data blocks used in these steps are formed from the division of a larger block; however, the division of that block does create two separate data blocks and hence the operation of Matsui does teach a data block that is encrypted with a key that is chosen dependently upon a previous data block.

Applicant also traverses this assertion.

First, even assuming *arguendo* that the more and less significant portions of the 8-bytes of input data 3 may be equated to message data blocks, it is clear that neither of these portions may be considered to be previous or subsequent to the other. In particular, and as the Advisory action admits, both of these portions are derived from common input data 3 – identified as an input "larger block". When the input "larger block" is received, both the more and less significant portions are processed at the same time. Accordingly, the more significant portion of input "larger block" 3 cannot be labeled as either previous or subsequent to the less significant portion. Applicant submits that another 8-bytes of input data 3 received by the Matsui system may properly be considered to be "*subsequent*" to a previously received 8-bytes of input data 3, however, each 8-bytes of input data 3 is processed by the Matsui system completely independent of the content of any other 8-bytes of input data 3. For at least this reason, Matsui fails to disclose each of the limitations of present claim 1.

Second, the Advisory action argues the 8-bytes of input data 3 corresponds to an input "larger block", and that this "larger block" is divided into other data blocks. Applicant submits interpreting the more and least significant portions of the input "block" as separate message data blocks, one of which is scrambled on the basis of the content of the other is also without merit. Matsui clearly discloses its process in terms of 8-bytes of cleartext input data 3 and 8-bytes of scrambled text output data 4. Matsui merely scrambles the less significant bytes of the input data 3 with a key selected based upon its content, exclusive OR's the resultant with the more significant bytes of the input data 3, and the then resultant and less significant bytes of the input data 3 are transposed. *See, e.g., Matsui, col. 5, line 67 – col. 6, line 16.* The transposed resultant and less significant bytes are then subjected to analogous processing in processing block 10. Again, Matsui merely scrambles the less significant bytes of the previous processing resultant with a key selected based upon its content, exclusive OR's the resultant with the more significant bytes of the previous processing resultant, and the then resultant and less significant bytes of the previous processing resultant are again transposed. *See, e.g., Matsui, col. 5, lines 17-35.* This processing is repeated for some predetermined number of times to provide a scrambled output data 4 responsively to a cleartext input data 3.

Thus, Matsui teaches processing cleartext input data 3 as a single block and at each processing block, e.g. 9, 10, 11, 16 - - not processing a subsequent message data block based upon the data content of a previous message data block.

VIII CONCLUSION

Claim 1 recites a method to encrypt a data message having a plurality of message data blocks prior to transmitting said message data blocks over a network. The recited method includes extracting a data value from one of the message data blocks; selecting an encryption key from among a plurality of encryption keys dependently upon the extracted data value; and, encrypting a subsequent one of the message data blocks using the selected encryption key. In contradistinction, Matsui teaches a method where 8-bytes of input cleartext data is scrambled using keys selected on the basis of its own content, to provide 8-bytes of output scrambled data.

Accordingly, Matsui clearly fails to teach the claimed method and thus fails to anticipate Claim 1. That is, Matsui fails to teach all of the limitations of independent Claim 1, in at least that it fails to teach: (1) extracting a data value from one of the message data blocks; (2) selecting an encryption key from among a plurality of encryption keys dependently upon the extracted data value; and, (3) encrypting a subsequent one of the message data blocks using said selected encryption key. Accordingly it is respectfully submitted that the rejection of Claim 1 should be reversed.

Respectfully submitted,

By: ____________ RN 42,670
Plevy, Howard & Darcy, PC
(215) 542-5824

APPENDIX I - APPEALED CLAIMS

1. A method to encrypt a data message having a plurality of message data blocks prior to transmitting said message data blocks over a network, said method comprising:

extracting a data value from one of said message data blocks;

selecting an encryption key from among a plurality of encryption keys dependently upon said extracted data value; and,

encrypting a subsequent one of said message data blocks using said selected encryption key.

APPENDIX II - TABLE OF CASES

Glaverbel Societe Anonyme v. Northlake Marketing & Supply, Inc., 45 F.3d 1550, 33 U.S.P.Q.2d 1496, 1498 (Fed. Cir. 1995)

Richardson v. Suzuki Motor Co., 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989)

Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987)

APPENDIX III - LIST OF REFERENCES

U.S. Pat. No.	Issued Date	102(e) Date	Inventor
5,488,661	Jan. 30, 1996	Jun. 9, 1992	Matsui

TABLE OF CONTENTS

APPENDICES